УДК 342.9:004.056.53:327.8(470:477)

**КРАСНОСТУП Г.М.,** *кандидат юридичних наук, старший науковий співробітник,* провідний науковий співробітник наукової лабораторії інформаційного права та інформаційної безпеки Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України».
ORCID: https://orcid.org/0009-0002-8074-3383

# НОВА СТРАТЕГІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПРАВОВА ВІДПОВІДЬ НА РОСІЙСЬКЕ ІНФОРМАЦІЙНЕ МАНІПУЛЮВАННЯ ТА ВТРУЧАННЯ

DOI: https://doi.org/10.37750/2616-6798.2025.2(53).334149

***Анотація.*** *Ця стаття розглядає необхідність нової Стратегії інформаційної безпеки, враховуючи безпрецедентні виклики повномасштабної російської агресії. Аналізуються чинні правові рамки, висвітлюючи їхні недоліки на тлі динамічних загроз гібридної війни, зокрема поширення дезінформації через приватні месенджери та її вплив на національну ідентичність. Дослідження обґрунтовує введення терміну RIMI (російське інформаційне маніпулювання та втручання) як окремого поняття, підкреслюючи унікальний та системний характер агресивної інформаційної війни Росії. Цей специфічний фокус є вирішальним для України у розробці адекватних контрстратегій та для міжнародної спільноти у точному визначенні актора загрози. У статті детально описано як глобальні, так і національні виклики інформаційній безпеці, включно з маніпуляціями за допомогою ШІ, недостатньою медіаграмотністю та інформаційним домінуванням Росії на окупованих територіях. Зрештою, запропоновані вісім стратегічних цілей, спрямованих на комплексний захист інформаційного простору України та зміцнення її національної безпеки.*

***Ключові слова:*** *інформаційна безпека, стратегія, правові аспекти, іноземні інформаційні маніпуляції та втручання, дезінформація.*

***Summary.*** *This article examines the need for a new Information Security Strategy, given the unprecedented challenges of Russia's full-scale aggression. It analyses existing legal frameworks, highlighting their shortcomings against the dynamic threats of hybrid warfare, particularly the spread of disinformation via private messengers and its impact on national identity. The study advocates for introducing RIMI (Russian Information Manipulation and Interference) as a distinct term, emphasizing the unique and systemic nature of Russia's aggressive information warfare. This specific focus is crucial for Ukraine to develop adequate counter-strategies and for the international community to precisely identify the threat actor. The article details both global and national information security challenges, including AI-driven manipulation, insufficient media literacy, and Russia's information dominance in occupied territories. Ultimately, the proposed eight strategic goals aim to comprehensively protect Ukraine's information space and strengthen its national security.*

***Keywords:*** *information security, strategy, legal aspects, foreign information manipulation and interference, disinformation.*

***Постановка проблеми.*** Забезпечення інформаційної безпеки України є однією з ключових функцій держави, особливо в умовах триваючої збройної агресії з боку Російської Федерації. Повномасштабне вторгнення Російської Федерації, яке розпочалося 24 лютого 2022 року, стало третім етапом розв’язаної Росією ще у 2014 році російсько-української війни, участь у якій Російська Федерація намагалася заперечувати. Генеральна Асамблея ООН у своїй резолюції від 02 березня 2022 року

офіційно визнала ці дії як агресію проти України, а Міжнародний суд ООН 16 березня 2022 року зобов'язав Росію припинити воєнні дії. Незважаючи на це, війна триває, і одним із її інструментів є масштабне поширення дезінформації, проведення інформаційних та психологічних операцій та інших форм ворожого інформаційного впливу.

Статтею 2 Указу Президента України від 28 грудня 2021 року № 685/2021 затверджено Стратегію інформаційної безпеки [1]. Повномасштабне вторгнення перетворило інформаційний простір на повноцінний фронт бойових дій, де інформація є зброєю, а не лише інструментом впливу. Це вимагає абсолютно інших підходів до захисту та наступу в інформаційній сфері. Тому Стратегія була актуальною на момент розробки, та повномасштабне вторгнення Росії 24 лютого 2022 року принципово змінило характер загроз та викликів, зробивши її положення значною мірою застарілими та недостатніми.

Слід зазначити, що правовою основою Стратегії є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392 [2], а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Загрози інформаційній безпеці набули екзистенційного характеру, спрямовані на знищення української державності, української національної та громадянської ідентичності та єдності. Це потребує не просто протидії, а формування стійкого інформаційного імунітету суспільства.

Росія значно посилила інформаційні маніпуляції та втручання, у тому числі шляхом поширення дезінформації та пропаганди, реалізації спрямованих на деморалізацію українців інформаційних кампаній, підрив довіри до влади, поширення паніки, а також дискредитацію України на міжнародній арені. Обсяги та складність цих операцій багаторазово зросли.

Такі платформи як Telegram, WhatsApp, інші приватні месенджери стали ключовими каналами для поширення дезінформації та психологічних операцій, що не було повною мірою враховано у попередній стратегії. Це вимагає нових підходів до регулювання та співпраці з платформами.

Інформаційні атаки тепер тісно інтегровані з військовими операціями, що дозволяє ворогу використовувати їх для створення "інформаційного туману війни", маніпуляцій та підготовки до реальних бойових дій. При цьому, під "інформаційним туманом війни" ми пропонуємо розуміти невизначеність і відсутність чіткої інформації про ситуацію на фронті або в зоні конфлікту, що використовується для заплутування противника та зміцнення своєї позиції. Росіяне навмисно створюють умови для заплутування, маніпулювання або для захисту від витоків стратегічно важливої для них інформації.

Ця стаття ставить перед собою завдання ретельно проаналізувати правові аспекти визначення актуальних викликів та загроз національної безпеки України в інформаційній сфері, стратегічних цілей та завдань, спрямованих на протидію цим загрозам, захист прав осіб на інформацію. Особлива увага буде приділена напрацюванню пропозицій до нової редакції Стратегії інформаційної безпеки.

***Результати аналізу наукових публікацій***. У своїх наукових працях проблемні питання регулювання суспільних відносин щодо інформаційної безпеки держави досліджують такі вітчизняні науковці: І. В. Арістова, О. А. Баранов, П. Д. Біленчук, В. М. Брижко, О. Є. Бухтатий, О. А. Вознесенська, А. В. Войціховський, А. Г. Гетьманець, В. М. Дрешпак, І. В. Зайцева-Калаур, Т. А. Костецька, А. Ю. Нашинець-Наумова, А. М. Новицький, О. М. Селезньова, М. А. Рожило,

О. Л. Теребус та інші. Окремо хочу виділити колег, які внесли вагомий внесок у правове регулювання суспільних відносин з питань забезпечення інформаційної безпеки, а саме: К. І. Бєляков, Д. В. Дубов, О. О. Золотар, В. С. Цимбалюк.

Разом з цим, потребує додаткового дослідження та висвітлення питання визначення на законодавчому рівні актуальних викликів та загроз національній безпеці України в інформаційній сфері, стратегічних цілей та завдань, спрямованих на протидію цим загрозам, захист прав осіб на інформацію.

***Метою статті*** є обґрунтування доцільності розробки нової Стратегії інформаційної безпеки України та формування конкретних пропозицій до її змісту, виходячи з аналізу актуальних правових викликів та загроз, спричинених повномасштабною російсько-українською війною та безпрецедентним російським інформаційним маніпулюванням та втручанням (RIMI).

***Виклад основного матеріалу***. Сьогодні ключовим документом з підготовки стратегій є Закон України "Про правотворчу діяльність" та Регламент Кабінету Міністрів України, затверджений постановою Кабінету Міністрів України від 18 липня 2007 року № 950 (у редакції постанови Кабінету Міністрів України від 9 листопада 2011 року № 1156).

Пунктом 2 частини другої статті 23 зазначеного Закону стратегії віднесено до програмних документів публічної політики, які приймаються для розроблення документів прогнозування розвитку країни, окремого виду суспільних відносин на довготривалий період та способів досягнення поставленої мети [3].

Відповідно до § 57 Регламенту стратегія визначає курс формування та реалізації політики у відповідних сферах на середньостроковий або довгостроковий період та повинна містити:

опис проблем, які обумовили її прийняття, і нормативно-правових актів, що діють у відповідних сферах;

аналіз поточного стану справ, тенденції та обґрунтування щодо необхідності розв'язання виявлених проблем;

стратегічні цілі та показники їх досягнення;

завдання, спрямовані на досягнення поставлених цілей, етапи їх виконання, очікувані результати на кожному етапі, з відображенням запланованого темпу досягнення цільових показників та орієнтовного обсягу необхідних фінансових, матеріально-технічних, людських та інших ресурсів;

порядок проведення моніторингу, оцінки результатів реалізації стратегії та звітування;

операційний план реалізації стратегії на трирічний період [4].

Підготовці нової редакції Стратегії інформаційної безпеки має передувати глибинний аналіз та актуалізація загроз та викликів інформаційній безпеці, які умовно можна поділити на глобальні та національні.

На цьому етапі дослідження пропонуємо визначити глобальні загрози та виклики.

В першу чергу це збільшення кількості глобальних дезінформаційних кампаній

Глобальні дезінформаційні кампанії, що активно інспіруються авторитарними урядами, зокрема Російською Федерацією, а також радикальними рухами, стали повсякденною практикою. Їхня мета – маніпулювання громадською свідомістю, розпалювання недовіри, посилення внутрішньої поляризації та дестабілізація демократичних суспільств. Такі кампанії становлять реальну загрозу демократичному розвитку держав, міжнародній стабільності та верховенству права.

Інформаційна політика Російської Федерації як загроза не лише Україні, а й іншим демократичним державам

Із початком повномасштабного вторгнення 24 лютого 2022 року інформаційна агресія Російської Федерації набула системного та тотального характеру. Спеціальні інформаційні операції ворога спрямовані проти ключових демократичних інституцій, включаючи вибори, медіа, правозахисні організації та громадянське суспільство. Спецслужби держави-агресора свідомо розпалюють внутрішні протиріччя в Україні та інших державах, прагнучи послабити їхню стійкість зсередини.

Інформаційний вплив на противника – складова бойових дій. Розпочавши широкомасштабну збройну агресію проти України, Російська Федерація веде бойові дії одночасно на землі, у повітрі, на морі, у кіберпросторі, а також економічній, політико-дипломатичній та інформаційній сферах. При цьому Російська Федерація розглядає інформаційний вплив на противника як невід'ємну складову бойових дій. Для просування потрібних наративів Російська Федерація активно використовує як медіа, соціальні мережі, так і вище політичне керівництво та представників органів влади, російський дипломатичний корпус, громадські організації, співробітників російських культурних центрів, митців. Для просування пропаганди Російська Федерація також активно залучає іноземних політиків, журналістів, лобістів та навіть глав окремих держав.

Застосовані державою-агресором технології гібридної війни проти України – включно з інформаційними операціями, кампаніями з маніпуляції фактами, дискредитацією інституцій та розпалюванням ворожнечі – активно експортуються до інших країн і швидко адаптуються до місцевих контекстів. В умовах недостатнього регулювання онлайн-простору ці загрози масштабуються. Однією з відповідей на дезінформаційну активність держави-агресора є санкції та ефективний міжнародний механізм моніторингу дотримання обмежувальних заходів.

Міжнародний характер загроз інформаційної безпеки зумовлює необхідність вироблення спільної стратегії інформаційної безпеки і розвиток міждержавного співробітництва в рамках міжнародних організацій у зазначеній сфері [5, С. 287].

18 липня 2022 року Рада Європейського Союзу схвалила висновки щодо іноземного інформаційного маніпулювання та втручання (далі – FIMI), згідно з якими вторгнення Росії в Україну та її воєнна пропаганда підкреслили нагальність боротьби з маніпуляціями та втручанням іноземною інформацією, спрямованими не лише на російську, а й на світову аудиторію [6]. У висновках підкреслюється, що іноземні інформаційні маніпуляції та втручання часто використовуються як частина ширших гібридних кампаній та спрямовані на введення в оману, обман та дестабілізацію демократичних суспільств шляхом створення та використання культурних та соціальних суперечностей стратегічним та скоординованим чином. Також Висновки демонструють зобов'язання ЄС посилити свою участь у боротьбі з цією загрозою на всіх рівнях, зокрема в багатосторонніх форматах з Організацією Об'єднаних Націй та іншими міжнародними та регіональними організаціями та в їх рамках. Рада Європейського Союзу закликає всі відповідні сторони активізувати роботу з розробки міжнародних принципів щодо дезінформації та FIMI.

FIMI часто використовується як частина ширших гібридних кампаній і, серед іншого, спрямована на введення в оману, обман та дестабілізацію наших демократичних суспільств, створення та експлуатацію культурних та соціальних тертя, а також негативний вплив на нашу здатність проводити зовнішню та безпекову політику. Наголошує, що стратегічне та скоординоване використання інформації, маніпуляції та

втручання з боку Росії, що передувало та супроводжує неспровоковану та невиправдану військову агресію проти України, ілюструє цю багатогранну загрозу з її конкретним впливом на різні сфери внутрішньої та зовнішньої політики.

Європейська служба зовнішніх справ (EEAS), яка є одним з ключових гравців у моніторингу та аналізі FIMI, де Росія часто фігурує як головний актор, регулярно публікує звіти про FIMI. У цих звітах Росія, поряд з Китаєм, постійно виділяється як основне джерело таких загроз. Наприклад, у третьому звіті EEAS про FIMI прямо зазначається, що цифрова інфраструктура розгортається іноземними акторами, "переважно Росією, а також Китаєм". Це демонструє фокус на російській діяльності. У березні 2025 року EEAS оприлюднила третій звіт, у якому у тому числі йдеться про загрози RIMI [7].

Стратегічний компас, ухвалений ЄС у березні 2022 року, визначає план дій для посилення політики Європейського Союзу у сфері безпеки та оборони до 2030 року [8]. Одним із аспектів, охоплених у контексті політики безпеки, є розробка Інструментарію протидії іноземному інформаційному маніпулюванню та втручанню FIMI. Цей інструментарій є каталогом засобів, багато з яких перебувають у постійній імплементації, для боротьби з операціями FIMI та реагування на них.

Такі організації, як Атлантична рада (Atlantic Council), Debunk.org, Африканський центр стратегічних досліджень (Africa Center for Strategic Studies) та інші, публікують численні матеріали, які детально аналізують саме російські кампанії з інформаційного впливу, їхні тактики, цілі та наслідки в різних регіонах світу (Балтія, Центральна Азія, Африка, країни "Люблінського трикутника" тощо). Вони часто використовують термінологію "російська дезінформація", "кремлівські інформаційні маніпуляції" або "російське іноземне втручання".

Африканський центр стратегічних досліджень (Africa Center for Strategic Studies) у травні 2025 року оприлюднив інтересну статтю на тему "Російська кампанія впливу в Африці використовує "репортерів-примар", в якій наведено результати розслідування щодо RIMI в Африці. Так, політичний та військовий аналітик Грегуар Сиріль Донгобада за два з половиною роки опублікував понад 75 статей, у яких розповідається про понад десяток країн Західної Африки.

Родом з Центральноафриканської Республіки, він зараз мешкає в Парижі. Донгобада використав свій експертний аналіз, щоб зосередитися на ролі Франції та Росії в африканському секторі безпеки, публікуючи такі заголовки, як "Причини антифранцузьких настроїв у Західній Африці" та "Заздрість Франції до успіхів російської присутності в Малі". Однак є проблема: Грегуара Сиріля Донгобади не існує.

Нещодавнє розслідування "репортерів-примар", проведене Al Jazeera, виявило понад 15 авторів, чиї імена з'являлися щонайменше у 200 статтях з 2021 року у виданнях по всій Західній Африці. Статті відповідають відомому профілю російської пропаганди, яка критикує Францію та Організацію Об`єднаних Націй, водночас прославляючи присутність російських найманців.

Так званий аналітик Донгобада з'являється нізвідки у лютому 2021 року, – повідомила "Аль-Джазіра". Немає жодних записів про його освіту, жодних ознак його зв'язку з аналітичними центрами чи університетами, а також жодної трудової історії. Для свого репортажу "Аль-Джазіра" проаналізувала фотографії, використані Донгобадою в соціальних мережах, і виявила, що вони збігаються з фотографіями чоловіка з Центральної Африки на ім`я Жан-Клод Сендеолі, вчителя та футбольного арбітра, який помер у 2020 році.

Розслідування виявило мережу посередників, які відмивали гроші російської пропаганди та здійснювали платежі за розміщення контенту в африканських виданнях з фальшивими авторами, які виглядають як справжні місцеві жителі [11].

Тому, сьогодні ведення терміну RIMI (російське інформаційне маніпулювання та втручання) в науковий обіг є доцільним та обґрунтованим з кількох причин:

Існуючий ширший термін FIMI, хоч і є загальновизнаним, не відображає унікальних, системних та екзистенційних загроз, що походять саме від Російської Федерації. Російська агресія, особливо після 2014 року та повномасштабного вторгнення у 2022 році, показала якісно новий рівень інформаційної війни. Цей рівень вимагає специфічного підходу та термінології.

Російське інформаційне маніпулювання та втручання характеризується безпрецедентним масштабом, інтенсивністю та використанням широкого спектру інструментів – від державних медіа до приватних ботоферм, від кібератак до прямої пропаганди на окупованих територіях. Це не просто "один з" іноземних впливів, а скоординована стратегія, спрямована на дестабілізацію та знищення держав.

Російська інформаційна діяльність є не випадковою, а системною, централізованою та цілеспрямованою. Вона є невід`ємною частиною її зовнішньої політики та військової доктрини. Введення окремого терміну підкреслить цей факт і допоможе краще класифікувати її дії.

Використання терміну RIMI дозволятиме чітко ідентифікувати джерело загрози. Це важливо для міжнародної спільноти, яка має визнавати конкретного актора, що здійснює агресивні дії в інформаційному просторі.

Для України, яка є безпосередньою жертвою цієї агресії, розрізнення "російського" від загального "іноземного" інформаційного втручання є критично важливим для розробки адекватних стратегій протидії. Це дозволяє зосередити ресурси та зусилля на найбільш небезпечному векторі.

Введення RIMI дозволить науковцям більш точно аналізувати та класифікувати специфічні методи, цілі та наслідки саме російського інформаційного впливу, що сприятиме глибшому розумінню феномену та розробці ефективніших контрзаходів.

Таким чином, термін RIMI (російське інформаційне маніпулювання та втручання) є не просто новим поняттям, а важливим інструментом для більш точного та глибокого розуміння унікальної, системної та агресивної інформаційної діяльності Російської Федерації, що є ключовим для національної безпеки України та глобальної стабільності.

По-друге, до глобальних викликів та загроз можна віднести швидкий розвиток штучного інтелекту та відсутність ефективної взаємодії з цифровими платформами. Використання штучного інтелекту для створення та масштабного поширення дезінформації, діпфейк-контенту та генерації великого обсягу маніпулятивних повідомлень ускладнює верифікацію фактів та ідентифікацію джерел впливу. Алгоритмічні рішення, що лежать в основі цифрових платформ, можуть не лише сприяти поширенню шкідливого контенту, а й посилювати ефект інформаційних операцій.

Водночас механізми взаємодії держав з глобальними цифровими платформами залишаються недостатньо розвиненими. Відсутність прозорості у прийнятті модераційних рішень, неврегульованість відповідальності за дії алгоритмів, недоступність критичних даних для аналізу становлять серйозний виклик для побудови ефективної системи інформаційної безпеки як на національному, так і на міжнародному рівні.

По-третє, на глобальний рівень інформаційної безпеки впливає недостатній рівень медіаграмотності в умовах стрімкого розвитку цифрових технологій.

Еліна Вроблєвська та Беніаміно Ірді у своїй статті на тему "Як найкраще боротися з російськими інформаційними маніпуляціями? Латвія має відповіді" підкреслюють, що навчання громадськості медіаграмотності з часом створює стійке суспільство, що призводить до того, що населення зменшує ймовірність бути обманутим фейковими новинами, а вплив діяльності впливу мінімізується [9].

Розширення доступу до інформації в цифровому середовищі відбувається на тлі недостатнього рівня критичного мислення та медіаграмотності багатьох груп населення. Це створює сприятливий ґрунт для маніпуляцій, поширення фейків, деструктивної пропаганди, популяризації теорій змови та підриву суспільної довіри до інституцій. У контексті повномасштабної війни Росії проти України, яка супроводжується активним поширенням дезінформації з боку держави-агресора, медіаграмотність набуває критичного значення для збереження політичної стабільності, громадського порядку, єдності та стійкості суспільства.

Звісно перелік глобальних викликів та загроз є предметом широкої дискусії у колі експертів. Тому цей перелік може бути доповненим.

Щодо національних викликів та загроз слід зазначити наступне.

По-перше, це системна інформаційна агресія Російської Федерації проти України.

На сьогодні Російська Федерація застосовує всі наявні засоби впливу на Україну за всім спектром інформаційного протистояння. Активному інформаційному впливу піддаються: населення України, населення країн-партнерів та третіх країн, а також населення Російської Федерації. Такі дії країна-агресор здійснює з метою завдання максимальної шкоди, зниження оборонного та економічного потенціалу, зменшення міжнародної підтримки та підриву іміджу України. Метою таких дій Російської Федерації є формування прокремлівських оцінок ситуації в Україні, легітимізація російської присутності на тимчасово окупованих територіях та зменшення підтримки нашої держави на міжнародній арені, у тому числі й у контексті передачі Україні озброєння і військової техніки, а також обмеження його далекобійності. Перед міжнародною спільнотою та власним населенням агресію проти України керівництво Російської Федерації виправдовує "захистом життєво важливих інтересів Росії", "правом на самооборону", "загрозою можливого членства України в Північноатлантичному альянсі". Російська Федерація намагається дискредитувати вище військово-політичне керівництво, Сили оборони України, євроінтеграційний та євроатлантичний курс України, актуалізувати проблеми у соціально-економічній сфері, історичні протиріччя з країнами-сусідами. Активно поширює так звані документальні матеріали про "порушення Україною міжнародного гуманітарного права".

Основними цілями держави-агресора залишаються підрив національної єдності, дискредитація української державності, послаблення довіри до демократичних інституцій, розпалювання соціальної напруги та деморалізація суспільства й оборонців України. Інформаційний вплив супроводжується кампаніями з демілітаризації західної допомоги Україні, делегітимації державної влади, нав'язування фальшивих наративів про "втому Заходу" та "невиправданість опору". Застосовуються гібридні інструменти впливу, зокрема підконтрольні медіа, бот-мережі, пропагандисти, використання штучного інтелекту для генерації діпфейків.

По-друге, це інформаційне домінування Російської Федерації як держави-агресора на тимчасово окупованих територіях України.

На тимчасово окупованих територіях Росія створює ізольоване інформаційне середовище, що цілеспрямовано викривлює реальність. Російська Федерація посилює контроль над інформаційно-телекомунікаційною системою, а також блокує доступ жителів окупованих територій до українських медіа. Для пропагандистського впливу Російською Федерацією запущено мовлення російських каналів. В умовах інформаційного вакууму Російська Федерація нав'язує антиукраїнські наративи, переконує населення на тимчасово окупованих територіях України в начебто терористичному характері дій керівництва України, представляє агресію Російської Федерації щодо України як складову формування справедливого багатополярного світоустрою. Окупанти знищують все, що пов'язано з українською національною та громадянською ідентичністю: символіку, книги, топоніми, пам`ятники. На тимчасово окупованих територіях України Російська Федерація продовжує запроваджувати адміністрування за російськими стандартами, російську фінансово-банківську систему, відкривати представництва політичних партій, створювати інституції з виявлення і нейтралізації проукраїнських активістів, проводити "паспортизацію" та примусову мобілізацію громадян України до збройних сил Російської Федерації та інших військових формувань, чинити військові злочини, посилювати утиски і безкарно порушувати права і свободи громадян України, які перебувають на цих територіях. Російська Федерація намагається прискорити "асиміляцію" населення окупованих територій України, створювати підґрунтя для подальшої агресії проти нашої держави.

Здійснюється тотальний контроль над медіа, блокування українського контенту, репресії проти незалежних журналістів і громадян, які виявляють проукраїнську позицію. Діти й молодь стають особливо вразливими об'єктами для пропаганди та мілітаризації свідомості. Російська Федерація активно переозброює окуповану інфраструктуру потужними передавальними засобами, що ускладнює контрзаходи з боку України.

По-третє, на сьогодні наша держава має обмежені можливості реагувати на дезінформаційні кампанії. Україна залишається вразливою до цілеспрямованих дезінформаційних кампаній через відсутність інтегрованої та стійкої системи інформаційної безпеки. Деструктивна пропаганда, поширення дезінформації як ззовні, так і всередині України застосовуються державою-агресором з метою підриву стійкості суспільства та інформаційної дестабілізації держави.

Незважаючи на позитивні зрушення, зокрема створення Центру протидії дезінформації та Центру стратегічних комунікацій та інформаційної безпеки, спроможності державних інституцій щодо координації зусиль залишаються недостатніми. Не сформовано єдиної державної системи кризової комунікації, швидкого реагування на фейки, аналізу загроз та ефективної протидії транснаціональним інформаційним операціям.

По-четверте, маємо відзначити недосконалість системи державних стратегічних комунікацій. Процес формування системи державних стратегічних комунікацій триває, але все ще бракує горизонтальної координації між органами влади, сталих механізмів залучення громадянського суспільства, експертного середовища, медіа. Відсутність цілісної візії, проактивного контенту, ефективної роботи з міжнародною аудиторією ускладнює досягнення інформаційної переваги.

Зазначене послаблює можливості до розбудови комплексного стратегічного планування інформаційного потоку, здійснення системної комунікативної діяльності Кабінету Міністрів України, об'єднання всіх ключових суб'єктів у сфері інформаційних відносин, суб'єктів формування і реалізації державної політики щодо ефективного

захисту національного інформаційного простору, утвердження позитивного іміджу України, реалізації цілей захисту національної безпеки України в інформаційній сфері.

По-п’яте, важливим викликом є недосконалість регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів.

В Україні реалізовується кампанія Ради Європи “Журналісти мають значення”, що спрямована на підвищення рівня безпеки працівників медіа та інших медіа професіоналів, посилення спроможностей держави у сфері захисту свободи слова, а також створення сприятливого середовища для якісної журналістики. Разом з тим, рівень безпеки журналістів, забезпечення їхніх прав і правових гарантій залишається недостатнім.

Особливо гостро стоїть проблема захисту журналістів-розслідувачів, які піддаються тиску, погрозам, а в окремих випадках – фізичним нападам або незаконному стеженню. В умовах воєнного стану доступ до інформації ускладнений, а ризики для журналістської діяльності зростають, водночас механізми реагування на порушення прав журналістів досі не є достатньо ефективними або інституційно закріпленими. Крім того, залишаються виклики, пов’язані з недостатнім рівнем саморегуляції у медіасекторі.

Також до національних загроз та викликів слід віднести інформаційні атаки проти євроінтеграційного курсу України. Стратегічний курс України на набуття повноправного членства в Європейському Союзі та в Організації Північноатлантичного договору закріплено у Конституції України. У Стратегії національної безпеки України європейська та євроатлантична інтеграція визначена одним із пріоритетів національних інтересів і національної безпеки.

Попри високий рівень підтримки європейської інтеграції серед населення, Російська Федерація і проксі-гравці всередині країни намагаються дискредитувати стратегічний курс України. Через поширення фейків, маніпуляцій, “експертних” заяв підривається довіра до НАТО та ЄС, роздмухується страх перед реформами, створюються штучні протиріччя між державою і громадянами.

Окремо до національних викликів та загроз треба віднести нерівний доступ до інформації на місцевому рівні.

Інформаційні потреби громад на місцевому рівні часто залишаються незадоволеними через низку структурних, економічних та правових бар’єрів. Значна частина населених пунктів, особливо у віддалених, прифронтових та деокупованих районах, досі має обмежений доступ до якісного інтернет-зв’язку, що унеможливлює оперативне отримання достовірної інформації.

Місцеві медіа у багатьох громадах залишаються вразливими до політичного впливу з боку місцевих еліт, що знижує рівень неупередженості та довіри до таких джерел. Через брак фінансової незалежності, зокрема у зв’язку зі складною економічною ситуацією, відсутністю сталого рекламного ринку та припиненням підтримки з боку окремих міжнародних донорів, зокрема США, багато місцевих медіа, особливо на сході та півдні України, змушені припинити свою діяльність.

При цьому з січня 2025 року Сполучені Штати непомітно призупинили 90 відсотків фінансування розвитку України, включаючи гранти, які підтримували існування більшості незалежних редакцій країни. Незалежно від того, чи надходило воно безпосередньо через USAID, чи через партнерів, це фінансування зникло. Рішення щодо скорочення фінансової підтримки відбувається на тлі посилення Москвою своїх зусиль щодо дезінформації [10].

Крім того, в окремих громадах фіксуються випадки незаконних відмов у наданні публічної інформації на запити журналістів та громадян, що ще більше ускладнює доступ до важливої інформації про діяльність органів влади. Усе це сприяє поширенню дезінформації, чуток та викривлених наративів, роблячи місцеві громади вразливими до маніпулятивного впливу як зсередини країни, так і з боку держави-агресора.

Разом з цим, окремим викликом для інформаційної безпеки є недостатній рівень медіаграмотності суспільства для протидії інформаційним маніпулятивним впливам. В умовах повномасштабної війни та зростаючої кількості цифрових загроз, брак навичок критичного сприйняття інформації, розпізнавання дезінформації та інформаційних маніпуляцій посилює вразливість громадян до психологічного тиску, поширення паніки й підриву довіри до державних інституцій. Це створює сприятливе середовище для реалізації ворожих інформаційних операцій як усередині країни, так і ззовні, що становить пряму загрозу національній безпеці.

***Висновки.*** У повномасштабній гібридній війні, розв'язаній Російською Федерацією проти України, інформаційний простір став одним із ключових полів битви. Ця стаття підкреслила критичну необхідність перегляду та оновлення Стратегії інформаційної безпеки як невідкладної правової відповіді на безпрецедентні виклики та загрози. Аналіз показав, що чинні підходи є недостатніми в умовах динамічних загроз, зокрема масштабованих кампаній російського інформаційного маніпулювання та втручання (RIMI), що використовують найновіші технології, включаючи штучний інтелект та приватні месенджери.

Виявлені глобальні та національні виклики – від системної російської інформаційної агресії до проблем медіаграмотності та регулювання цифрових платформ – підтверджують, що інформаційна безпека України потребує комплексного та багаторівневого захисту. Важливість виділення саме RIMI полягає у визнанні Російської Федерації як основного актора, що цілеспрямовано і системно веде інформаційну війну, спрямовану на знищення української державності, національної ідентичності та підрив міжнародної підтримки.

Запропоновані вісім стратегічних цілей нової Стратегії інформаційної безпеки є відповіддю на ці виклики:

Розвиток системи державних стратегічних комунікацій забезпечить проактивне поширення українських наративів та зміцнення національної ідентичності.

Забезпечення протидії дезінформації та гібридним загрозам передбачає створення ефективних механізмів реагування та співпрацю з цифровими платформами.

Визнання культури елементом національної безпеки сприятиме збереженню історичної пам'яті та утвердженню українських цінностей.

Формування суспільства, стійкого до інформаційних маніпуляцій, можливе через підвищення медіаграмотності та критичного мислення.

Удосконалення механізмів захисту прав людини в інформаційній сфері гарантує свободу слова та доступ до достовірної інформації.

Реалізація заходів інформаційної реінтеграції забезпечить повернення українського інформаційного простору на тимчасово окуповані та деокуповані території.

Посилення міжнародного співробітництва є ключовим для обміну досвідом, протидії спільним загрозам та залучення підтримки.

Забезпечення інформаційної єдності українців за кордоном сприятиме збереженню їхньої ідентичності та стимулюватиме повернення в Україну для участі у відбудові.

Досягнення цих цілей, що вимірюватимуться чіткими показниками, забезпечить не лише ефективний захист національного інформаційного простору, а й стане

фундаментом для зміцнення національної безпеки України в цілому. Нова Стратегія має стати живим, адаптивним документом, що постійно оновлюватиметься відповідно до динаміки загроз та розвитку технологій, забезпечуючи правову відповідь на агресивні дії Російської Федерації та створюючи умови для перемоги України в інформаційній війні.

**Використана література**

1. Стратегія інформаційної безпеки : Указ Президента України від 28 грудня 2021 року № 685/2021. URL: // https://zakon.rada.gov.ua/laws/show/685/2021#n5.

2. Стратегію національної безпеки України : Указ Президента України від 14 вересня 2020 р. № 392/2020. URL: // https://zakon.rada.gov.ua/laws/show/392/2020#Text.

3. Про правотворчу діяльність : Закон України від 24 серпня 2023 року № 3354-IX. URL: https://zakon.rada.gov.ua/laws/show/3354-20#Text.

4. Регламент Кабінету Міністрів України : постанова Кабінету Міністрів України від 18 липня 2007 р. № 950 (у редакції постанови Кабінету Міністрів України від 9 листопада 2011 р. № 1156). URL: https://zakon.rada.gov.ua/laws/show/950-2007-п#Text.

5. Войціховський А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В.Н. Каразіна. Серія «ПРАВО»*. Випуск 29. 2020. С. 281-288. URL: //file:///C:/Users/TEST/Downloads/15648-Article%20Text-31804-1-10-20200718%20(1).pdf.

6. Council conclusions on Foreign Information Manipulation and Interference (FIMI) : Council of the European Union. – Brussels, July, 18, 2022. – URL: //data.consilium.europa.eu/doc/document/ST-11429-2022-INIT/en/pdf

7. On Foreign Information Manipulation and Interference Threats : 3rd European External Action Service Report. March, 2025. URL: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf.

8. A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security. URL: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf.

9. Elina Vrobļevska and Beniamino Irdi // What's the best way to deal with Russian information manipulation? Latvia has answers. May, 2025. URL: https://www.atlanticcouncil.org/blogs/new-atlanticist/whats-the-best-way-to-deal-with-russian-information-manipulation-latvia-has-answers/

10. Muhammad Tahir. What's the best way to deal with Russian information manipulation? Latvia has answers. April 15, 2025. URL: https://www.atlanticcouncil.org/blogs/new-atlanticist/whats-the-best-way-to-deal-with-russian-information-manipulation-latvia-has-answers/

11. Russian Influence Campaign in Africa Uses «Ghost Reporters». May 6, 2025. URL: https://adf-magazine.com/2025/05/russian-influence-campaign-in-africa-uses-ghost-reporters/

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~